State Information Technology Services Division

Interconnection Security Agreement - Agency

This Interconnection Security Agreement (Agreement) is entered into the _____ day of _______, 2011 by and between the State Information Technology Services Division (SITSD) and ____ (Customer).

INTRODUCTION

A. The State of Montana, Chief Information Officer (CIO) is responsible for establishing statewide policies for security of information technology. Through policy, the CIO has determined that the state shall follow the National Institute of Standards and Technology (NIST) security guidelines and the Federal Information Security Management Act (FISMA). Since SITSD maintains the State of Montana network (SummitNet) and enterprise systems, it must comply with the NIST guidelines.

B. One of the NIST requirements (see NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems) is that an interconnection security agreement must be signed with each entity having information systems outside of the authorization boundary and connections to SITSD information systems.

C. This Agreement meets the NIST requirement that an interconnection security agreement be signed with outside entities.

Based on the above, the parties agree as follows:

AGREEMENT

1. **Term.** This Agreement is a requirement for Customer’s use of SummitNet. The Agreement is effective the last date of signature and continues so long as the Customer uses SummitNet

2. **Termination for Cause with Notice to Cure Requirement.** SITSD may terminate this contract for failure of Customer to perform its duties after giving the Contractor written notice of the stated failure. The written notice must demand performance of the stated failure within a specified period of time of not less than 90 days. If the demanded performance is not completed within the specified period, the termination is effective at the end of the specified period.

3. **Security Requirements.** Service-specific security requirements may be described in the SITSD Service Catalog. Customer shall follow these requirements if using the service. After July 1, 2012, the Customer is also required to comply with the following security requirements:

    - Develop, implement, maintain, and use appropriate safeguards that reasonably prevent the misuse of information systems and appropriately protect the confidentiality, integrity, and availability of information systems.

- Ensure that any agent, contractor or subcontractor to whom the Customer provides access agrees in writing to the same restrictions and conditions that apply through this Agreement to the Customer.

- Ensure that any agent, contractor or subcontractor to whom it provides access to information systems agrees in writing to implement reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of the information systems.

- Maintain a security plan for its information system(s).

- Report security incidents that occur on the Customer's information systems that may affect State of Montana enterprise systems to the SITSD Service Desk within 24 hours of occurrence.

- Maintain audit events according to the Customer's policy and provide this information to SITSD upon request. These audit logs must be kept according to Customer's records retention policy.

- Develop and implement policies and procedures regarding the use of information systems that describes how users are to protect against intrusion, tampering, viruses, etc.

- Identify minimum security training requirements and provide minimum security training to staff that access information systems.

Enterprise security policies are posted at the Enterprise Information Systems Policy Instruments web site, **http://itsd.mt.gov/policy/policies/default.mcpx.**

4. **Access to records**. The Customer shall allow access to its applicable records so that SITSD may confirm if Customer is meeting its obligations under this Agreement.

5. **Indemnity and liability.** The Customer shall indemnify, defend and hold harmless SITSD from and against any and all claims, demands, or actions arising or resulting from the Customer's failure to perform its obligations under this Agreement, including but not limited to damages, costs, and attorney fees, provided such damage to property or injury to persons is caused in whole or in part by the negligent act, error, or omission of the Customer or any of its employees, agents, consultants, or subcontractors.

6. **Assignment**. Customer may not delegate its duties or assign its rights hereunder unless SITSD approves in writing.

7. **Entire Agreement**. This Agreement is the entire agreement between the parties. No statements, promises of inducements made by either party, or agents of either party, which are not contained in the written Agreement, are valid or binding. This Agreement may not be enlarged, modified or altered except if done in writing signed by the parties.

Signatures of Approval and Agreement Date

Customer: Agency Head or Designee:

Printed Name Title

________/________/_______________

Signature Date

SITSD: State Chief Information Officer:

Printed Name Title

________/________/_______________

Signature Date